

Serial No.: 09/774,429

Attorney's Docket No.:10559/340001/P9885

REMARKS

Claims 1-15 and 17-26 remain as previously presented, and no new claims have been added.

Claims 1-15 and 17-26 stand rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over U.K. Patent Application GB 2317792A to Minear et al. ("Minear") in view of the non-patent literature, "Implementing a Distributed Firewall" to Ioannidis et al. ("Ioannidis").

In view of the remarks herein, the applicant respectfully traverses the rejections and requests reconsideration for an expedited notice of allowance.

I. The Rejections under 35 U.S.C. 103(a)

Claims 1-15 and 17-26 stand rejected under 35 U.S.C. 103(a) based on the proposed combination of Minear and Ioannidis.

Claim 1

Claim 1 is patentable over the combination of Minear and Ioannidis at least because the office action fails to present a *prima facie* case of unpatentability.

According to MPEP 2142,

"To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. In re Vaack, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See

Serial No.: 09/774,429

Attorney's Docket No.: 10559/340001/P9885

MPEP § 2143 - § 2143.03 for decisions pertinent to each of these criteria.

The initial burden is on the examiner to provide some suggestion of the desirability of doing what the inventor has done. "To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." Ex parte Clapp, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985). See MPEP § 2144 - § 2144.09 for examples of reasoning supporting obviousness rejections.

Minear and Ioannidis, in the suggested combination, does not teach each and every limitation of claim 1.

Claim 1 recites:

"if said classification parameter is not available, and the IPsec traffic is encrypted then decrypting traffic in a decrypting forwarding element separate from the first classifying forwarding element after said traffic has passed through said classifying forwarding element, and determining the classification parameter for the IPsec traffic." (emphasis added).

In contrast, Minear teaches a firewall, which both classifies the packet and decrypts the packet. The Examiner correctly identifies that "Minear does not disclose that the decrypting forwarding element is separate from the classifying forward element" (page 3, 2<sup>nd</sup> ¶, lines 1-3). Ioannidis reference is then relied upon to allegedly teach the limitation.

Applicant respectfully traverses. In contrast to the

Serial No.: 09/774,429

Attorney's Docket No.: 10559/340001/P9885

present application, Ioannidis teaches implementing a distributed firewall, which requires three distinct components.

"To implement a distributed firewall, we need a security policy language that can describe which connections are acceptable, an authentication mechanism, and a policy distribution scheme. As a policy specification language, we use the KeyNote trust-management system. As an authentication mechanism, we decided to use IPsec for traffic protection and user/host authentication." (pg. 192, col. 1, 3<sup>rd</sup> ¶ - 4<sup>th</sup> ¶, line 2).

Thus, KeyNote trust-management system does not replace IPsec for traffic protection and user/host authentication, but is implemented in addition to IPsec authentication.

"Our prototype implementation uses the KeyNote trust-management system, which provides a single, extensible language for expressing policies and credentials. We also make use of the IPsec stack in the OpenBSD system to authenticate users, protect traffic, and distribute credentials. The distribution of credentials and user authentication occurs as part of the Internet Key Exchange (IKE) [12] negotiation." (pg. 191, 2<sup>nd</sup> col., 1<sup>st</sup> full ¶, lines 1-9).

In fact, Ioannidis explicitly teaches passing the KeyNote credential as a part of the IKE exchange while establishing a connection over IPsec. Therefore, the encrypted traffic must be both classified and decrypted before the KeyNote credential can be forwarded to the local host.

"In case of a connection coming in over IPsec, the remote user or host will have established an IPsec Security Association with the local host using IKE. As part of the IKE exchange, a KeyNote credential as

Serial No.: 09/774,429

Attorney's Docket No.: 10559/340001/P9885

shown in Figure 9 is provided to the local host." (emphasis added (pg. 196, 1<sup>st</sup> col., last ¶)).

Thus, the office action incorrectly represents Ioannidis as teaching "a distributed firewall system in which classifying and decrypting/processing are separate elements...(see Figure 1, and also page 193, column 1, 2<sup>nd</sup> and 3<sup>rd</sup> paragraphs)." (pg. 3, lines 7-8). While the Examiner's intent is not clear, the office action appears to suggest that "KeyNote" and "Verifier" represent the "classifying forward element" and the "decrypting forward element, separate from the first classifying forwarding element" (emphasis added). However, nowhere in the reference does Ioannidis teach that KeyNote checks for "classification parameters" or "decrypts" IPsec traffic as recited in claim 1. In fact, Ioannidis is silent as to the method by which IPsec authenticates users, protects traffic, and distributes credentials before providing the KeyNote credential to the local host. Therefore, the referenced portions or any other portions of Ioannidis do not teach or suggest using two separate elements to classify and decrypt IPsec traffic.

In addition, the proposed combination of Minear and Ioannidis fails to teach "providing the classification parameter to the first classifying forwarding element" as recited in claim 1. Minear teaches a firewall with a single element for classifying and decrypting IPsec traffic, as correctly identified by the Examiner. Since Minear does not teach the decrypting forwarding element separate from the first classifying forward element, Minear lacks the "first classifying forwarding element" to which the classification parameter is to be provided.

The addition of Ioannidis does not alleviate the deficiency of Minear. The office action alleges that "the classification

Serial No.: 09/774,429

Attorney's Docket No.:10559/340001/P9885

parameter is passed to the first classifying element (see Figure 1, and also page 193, column 1, 2<sup>nd</sup> and 3<sup>rd</sup> paragraphs)". Again, the Examiner's intent is unclear, but the office action seems to suggest that returning the "results" of the KeyNote evaluator to applications (Figure 1 and Pg. 193, 1<sup>st</sup> paragraph) allegedly is "providing the classification parameter to the first classifying forwarding element". However, the portions of Ioannidis reference cited in the office action only teach the KeyNote trust-management system, which does not impact the method of classifying and decrypting IPsec traffic. As stated above, the encrypted IPsec traffic, which includes the KeyNote credential, must be classified and decrypted before the KeyNote credential can be forwarded to the KeyNote evaluator. Furthermore, KeyNote credential is not a IPsec classification parameter as recited in claim 1. According to Ioannidis, KeyNote "policy and credentials contain predicates that describe the trusted actions permitted by the holders of specific public keys (otherwise known as principles)".

Ioannidis at best is silent to the method of classifying and decrypting IPsec traffic. As such, there is no factual evidence present anywhere in the teachings of Ioannidis to suggest that Ioannidis teaches using two separate elements to classify and encrypt IPsec traffic or that classification parameter is provided to the first classification forwarding element.

For at least these reasons, Minear and Ioannidis, in the suggested combination, do not teach each and every limitation of claim 1.

Independent of addressing each and every limitation of the claim, the office action fails to establish a *prima facie* case of obviousness by failing to provide factual evidence to suggest

Serial No.: 09/774,429

Attorney's Docket No.:10559/340001/P9885

a reasonable expectation of success when combining Minear and Ioannidis. First, the proposed combination lacks at least the "classifying forward element" and the "decrypting forward element, separate from the first classifying forwarding element". Second, the proposed combination of Minear and Ioannidis is directed to applying the KeyNote trust-management system, which is unrelated to the method of classifying and decrypting IPsec traffic as recited in claim 1. Therefore, there is no reasonable expectation of success because any combination of Minear and Ioannidis would result in something other than the claimed subject matter of the present application.

Finally, the office action fails to establish a *prima facie* case of obviousness by failing to provide factual evidence to suggest a desirability to combine the teachings of Minear and Ioannidis to produce the method of claim 1. The office action alleges that the combination of Minear and Ioannidis is obvious for the following reason:

"It would have been obvious to use a distributed firewall arrangement, such as that disclosed by Ioannidis, in the invention disclosed by Minear. The motivation for doing so would be to rectify a number of drawbacks typical of standard firewalls (enumerated on page 190, 2<sup>nd</sup> column through page 191, 1<sup>st</sup> column)."

Serial No.: 09/774,429

Attorney's Docket No.:10559/340001/P9885

However, the above reasoning to combine Minear and Ioannidis is improper because it does not address the claimed subject matter of the present application. The proposed combination extends Minear and Ioannidis in an unrealistic way, for which the references do not provide motivation. In fact the references teach away from this proposed extension. If the teachings of Minear could be modified to implement the distributed firewall of Ioannidis, only the KeyNote trust-management system would be provided to decentralize policy assertion without addressing IPsec traffic.

In contrast, the applicant recites classifying and decrypting IPsec traffic using two separate elements, which must be performed upstream of the KeyNote trust-management system. The proposed combination of Minear and Ioannidis fails to result in using two separate elements to classify and decrypt IPsec traffic, and consequently fails to teach or suggest the method of claim 1. For example, without having the two separate elements, there is no "first classifying forwarding element" to which the "classification parameter" is provided. Thus, there is no motivation to combine Minear and Ioannidis because the proposed combination rules out the claimed subject matter of the present application.

For at least these additional reasons, claim 1 is patentable over the combination of Minear and Ioannidis.

Serial No.: 09/774,429

Attorney's Docket No.:10559/340001/P9885

Claims 2-5

Claims 2-5 depend from claim 1, and are therefore patentable over the combination of Minear and Ioannidis for at least the same reasons as stated above with respect to claim 1.

Claims 6-10

Claim 6 includes features similar to those discussed above with respect to claim 1, and is therefore patentable over the combination of Minear and Ioannidis for at least the same reasons as stated above with respect to claim 1. Claims 7-10 depend from claim 6, and are therefore patentable for at least the same reasons.

Claims 11-15 and 17-26

Claim 11 includes features similar to those discussed above with respect to claim 1, and is therefore patentable over the combination of Minear and Ioannidis for at least the same reasons. Claims 12-15 and 17-26 depend from claim 11, and are therefore patentable over the combination of Minear and Ioannidis for at least the same reasons.

CONCLUSION

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue, or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be



Serial No.: 09/774,429

Attorney's Docket No.: 10559/340001/P9885


exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Claims 1-15 and 17-26 are in condition for allowance, and a notice to that effect is respectfully solicited. If the Examiner has any questions regarding this response, the Examiner is invited to telephone the undersigned at (858) 678-4311.

Please apply any other charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: July 5, 2005

  
for Scott C. Harris  
Reg. No. 32,030  
Attorney for Intel Corporation

Fish & Richardson P.C.  
PTO Customer Number: 20985  
12390 El Camino Real  
San Diego, CA 92130  
Telephone: (858) 678-5070  
Facsimile: (858) 678-5099

**WILLIAM E. HUNTER**  
**REG. NO 47,671**

10517051.doc